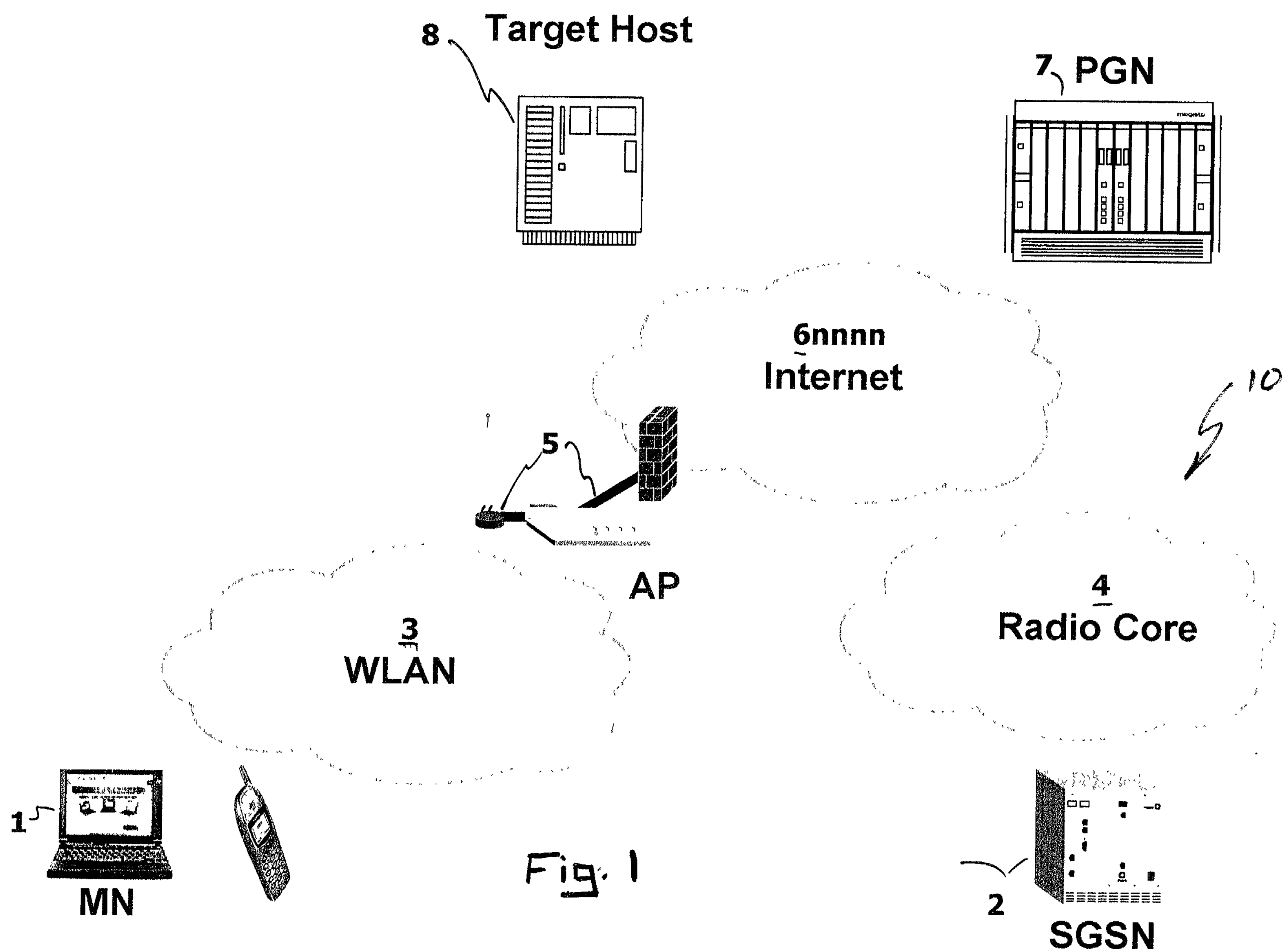
8
Target Host
7
PGN
6nnnn
Internet
10
5
AP
3
WLAN
4
Radio Core
1
MN
2
SGSN

Fig. 1

Phase 1

User Roams from GPRS to WLAN

1. MN has address of PGN and requests session key from PGN.

- PGN and MN exchange keying info using IKE, session keys for WLAN roaming are obtained.
- Luis prefers using something other than IKE (Kerberos).

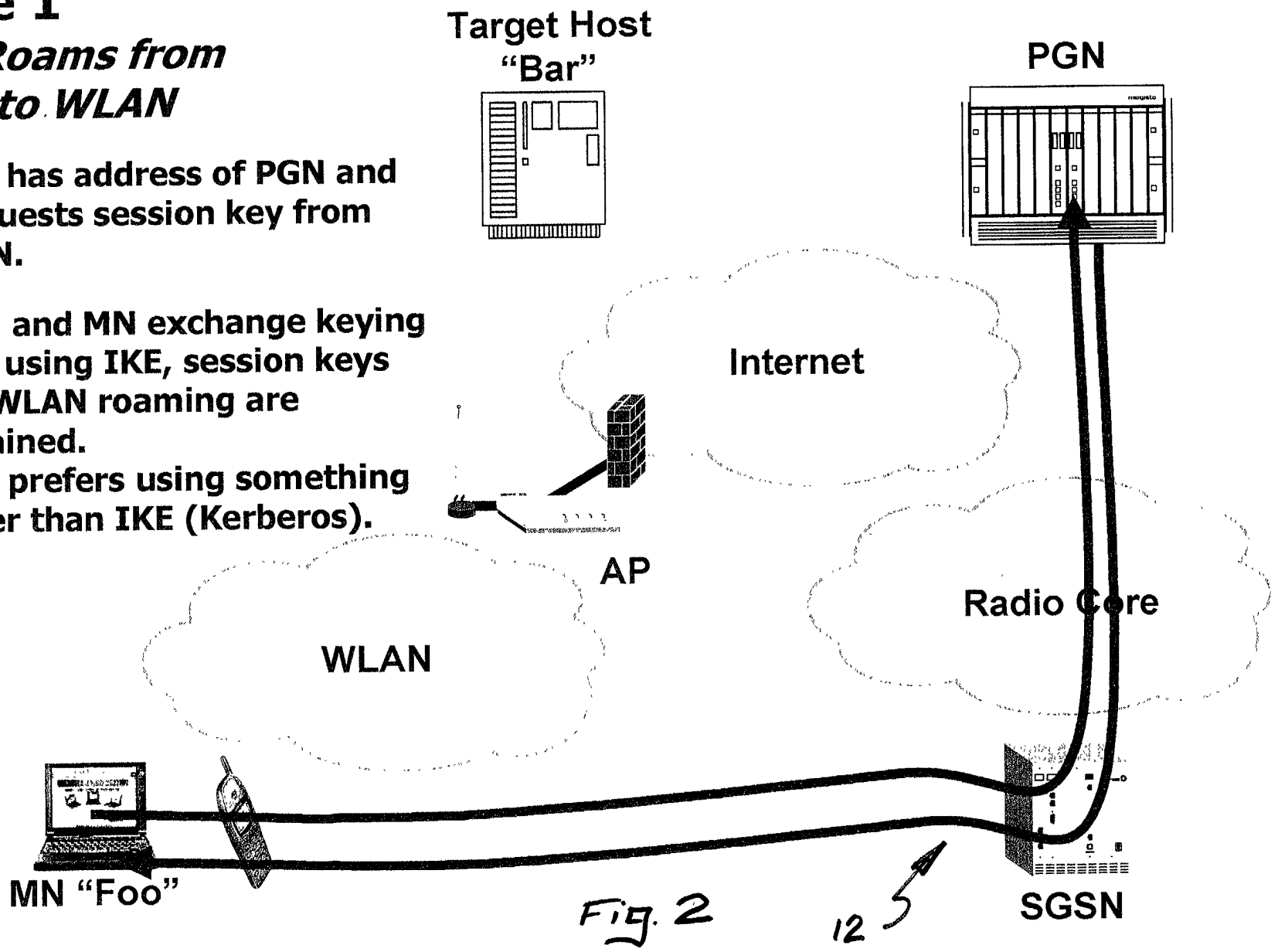

Fig. 2

12

Phase 2

1. MN shows up on WLAN and requests local care-of-address from DHCP
2. MN gets care-of-address

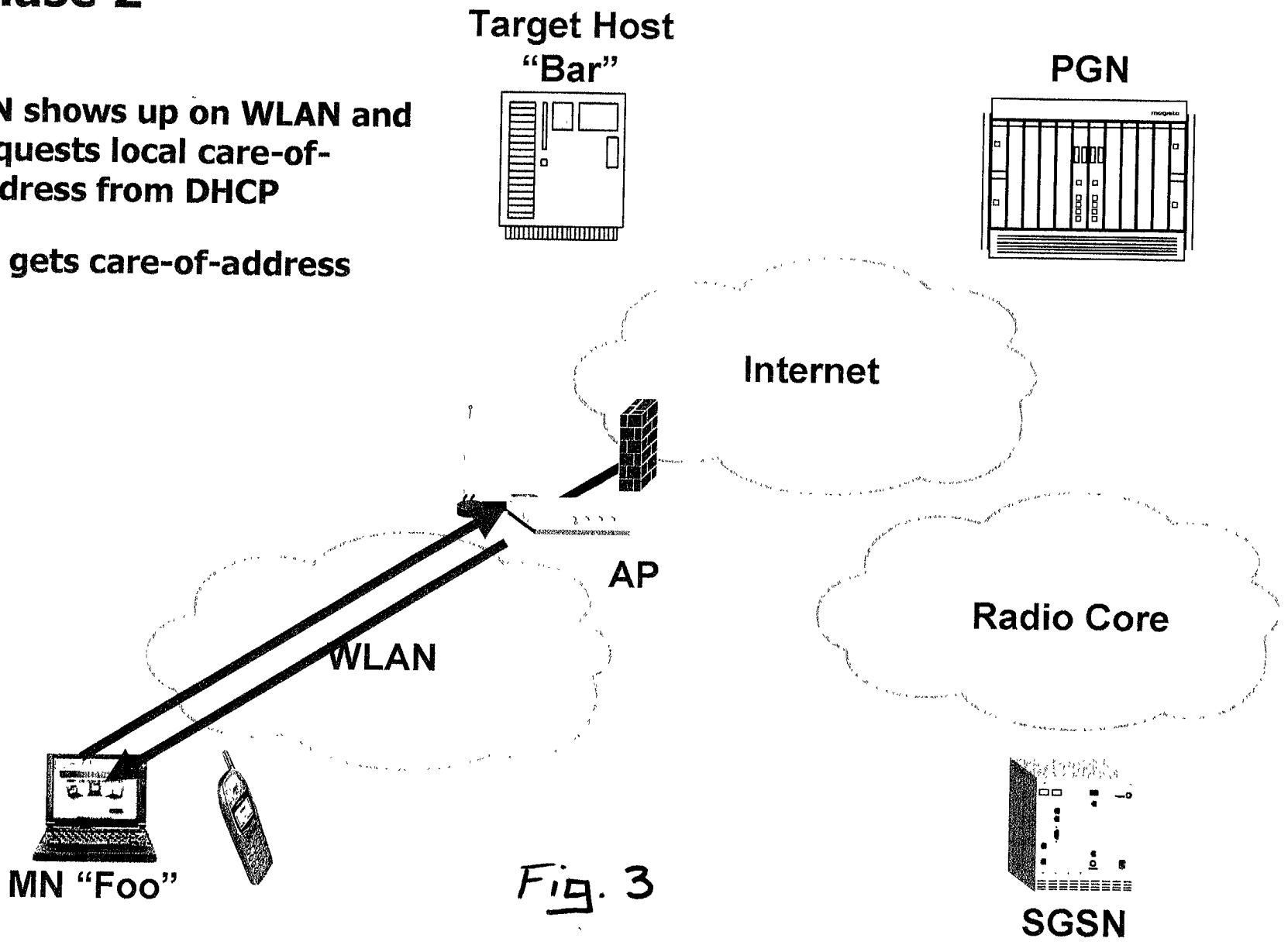

Fig. 3

Phase 3

1. MN sends a Mobile IP (MIP) registration request to the home agent (HA) hosted in the PGN

- HA sends registration reply (request and reply sent secured using session key)
- IKE used to set up IPSEC tunnel established between PGN and MN using COA (auth, encrypted, MICed)

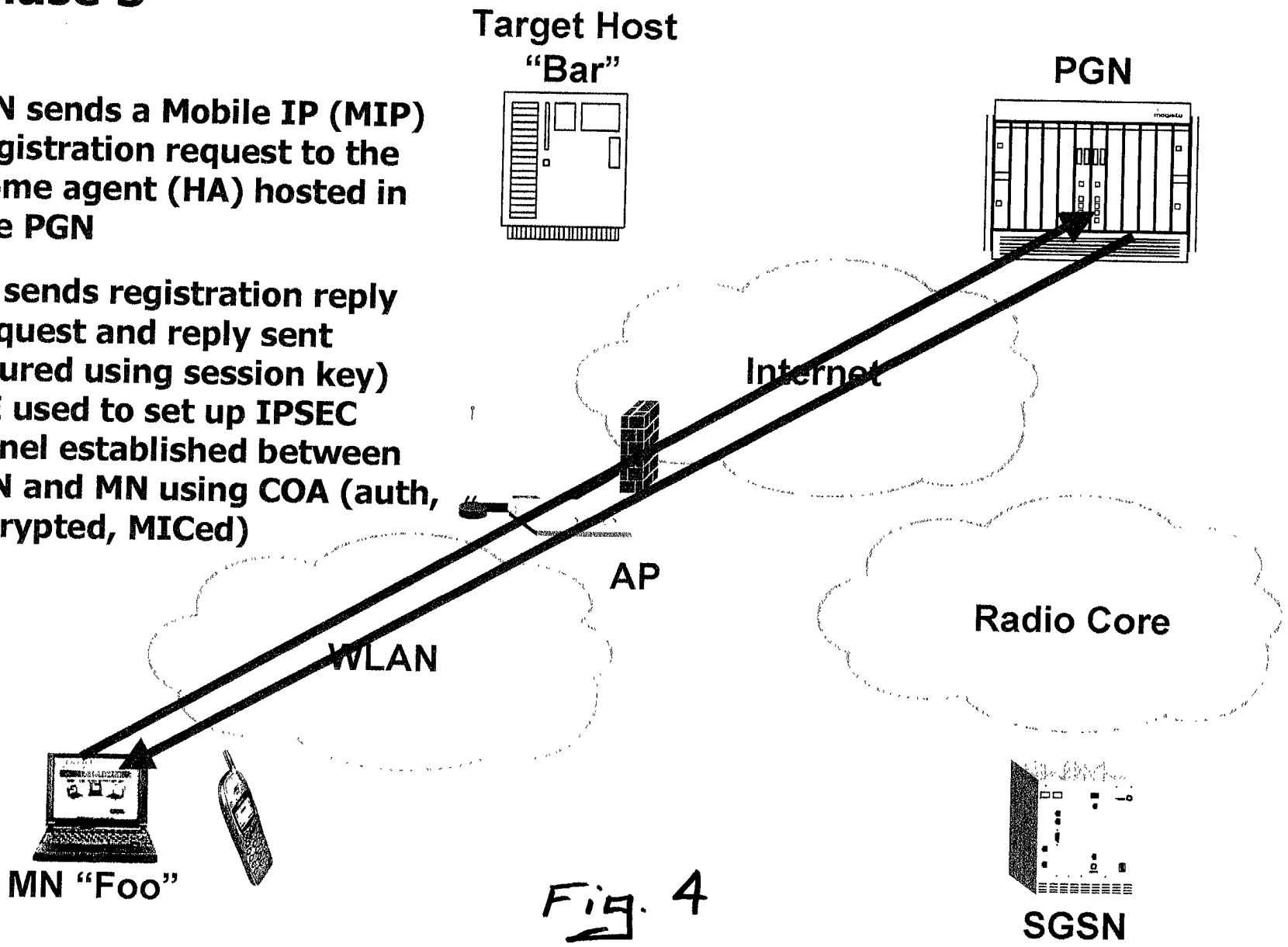

Fig. 4

Phase 4

1. MN Foo sends pkts to Bar via HA reverse IPSEC tunnel.

2. Bar sends packets to Foo via the HA in forward IPSEC tunnel.

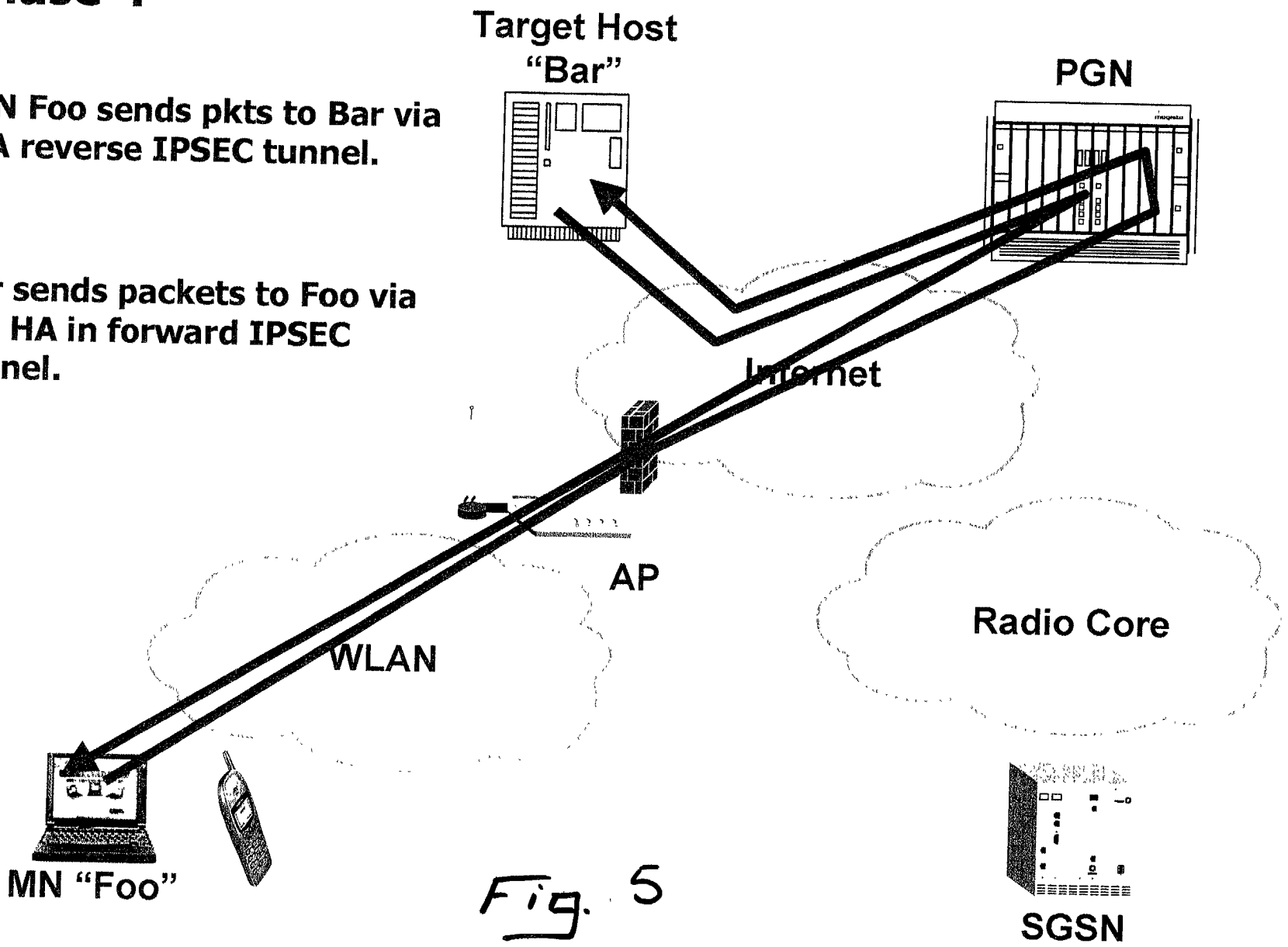

Fig. 5

Phase 5

User Roams from WLAN to GPRS

- MN foo sends MIP registration request to HA using authentication info generated from session key to say that it is back on home network.

2. HA sends MIP registration reply back to MN Foo.

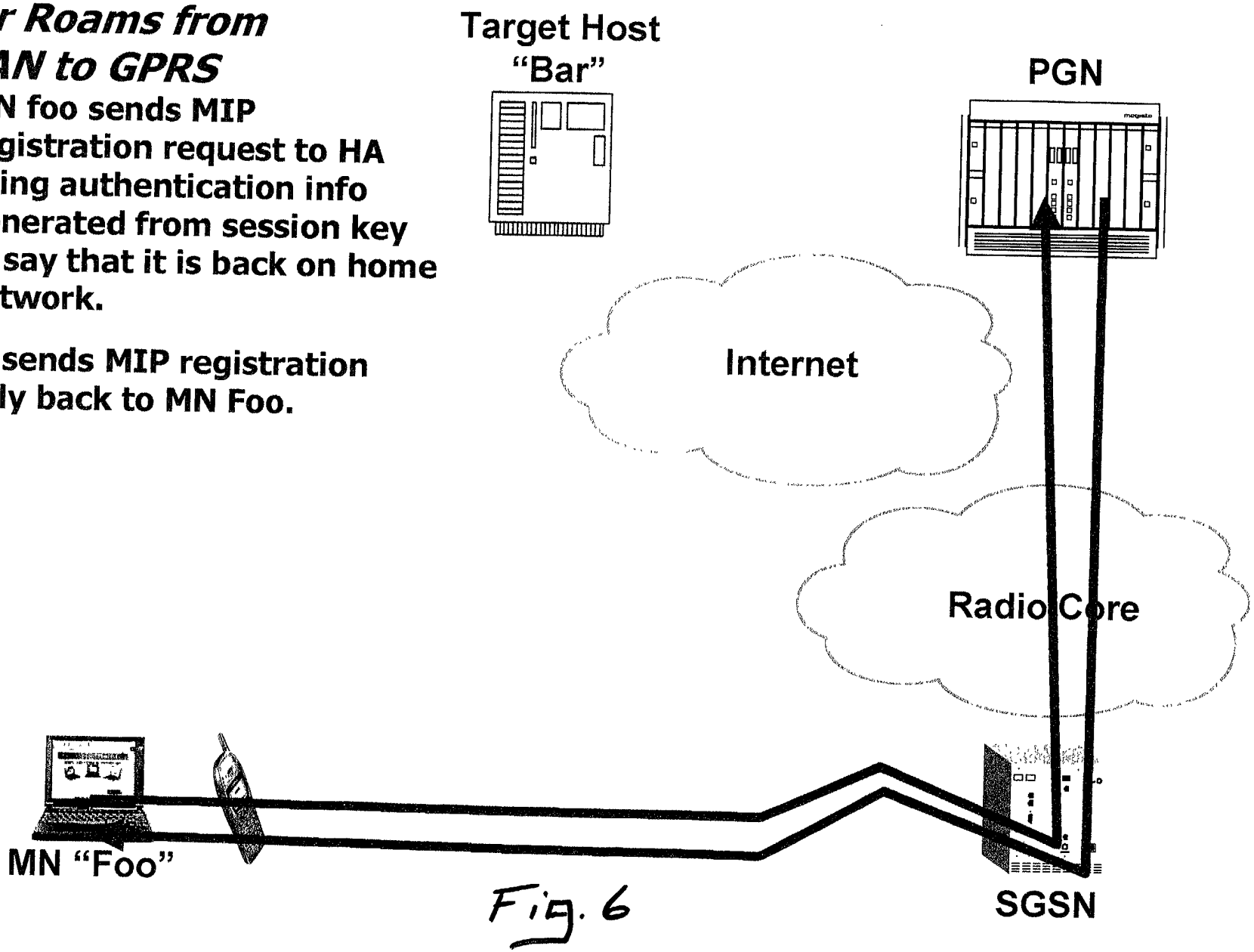

Fig. 6

Phase 6

1. Packets from Foo to Bar now go via GPRS only.

2. Packets from Bar to Foo now go via GPRS only.

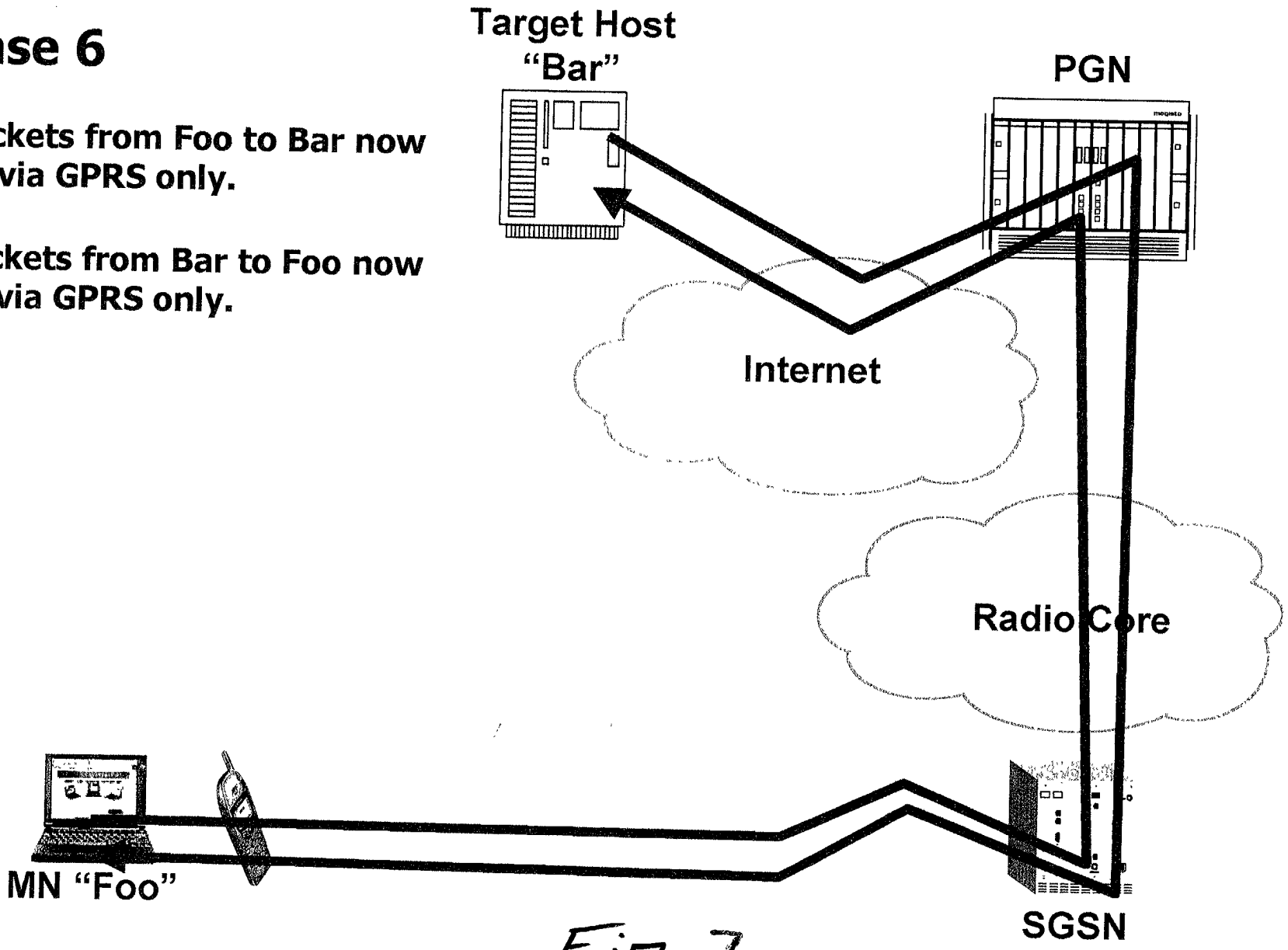

Fig. 7

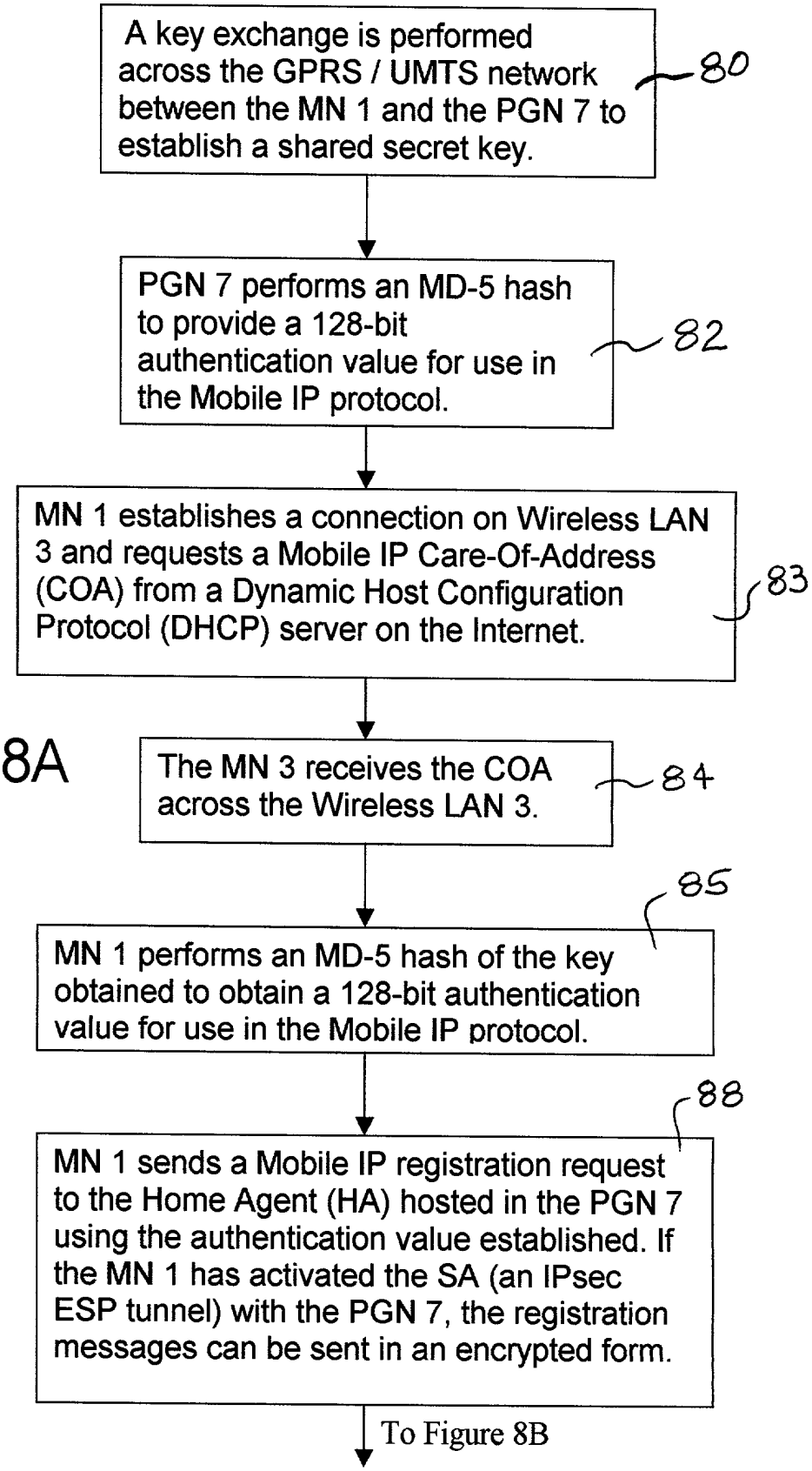
A key exchange is performed across the GPRS / UMTS network between the MN 1 and the PGN 7 to establish a shared secret key.
80
PGN 7 performs an MD-5 hash to provide a 128-bit authentication value for use in the Mobile IP protocol.
82
MN 1 establishes a connection on Wireless LAN 3 and requests a Mobile IP Care-Of-Address (COA) from a Dynamic Host Configuration Protocol (DHCP) server on the Internet.
83
The MN 3 receives the COA across the Wireless LAN 3.
84
MN 1 performs an MD-5 hash of the key obtained to obtain a 128-bit authentication value for use in the Mobile IP protocol.
85
MN 1 sends a Mobile IP registration request to the Home Agent (HA) hosted in the PGN 7 using the authentication value established. If the MN 1 has activated the SA (an IPsec ESP tunnel) with the PGN 7, the registration messages can be sent in an encrypted form.
88
To Figure 8B

Fig. 8A

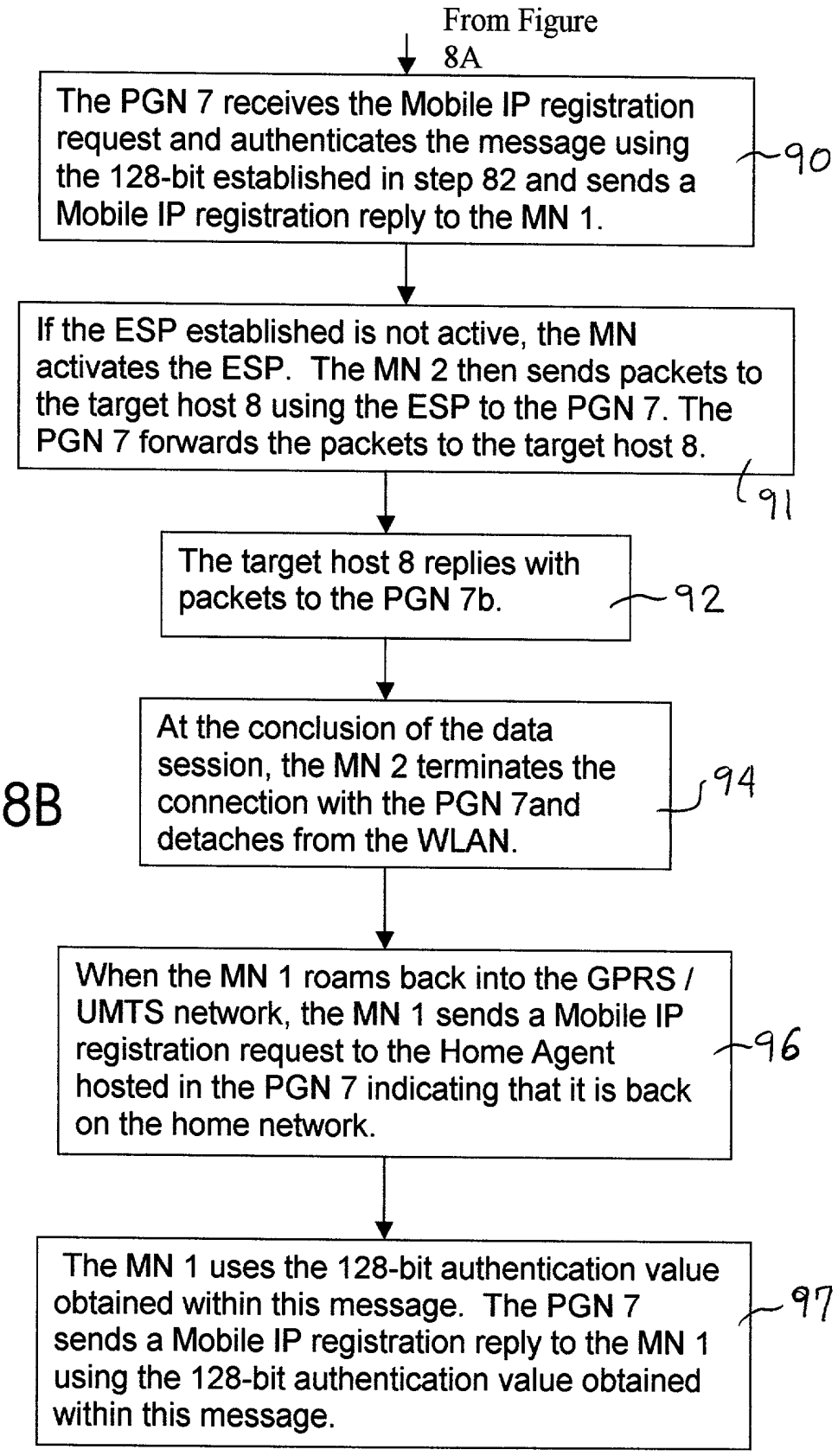
From Figure 8A
The PGN 7 receives the Mobile IP registration request and authenticates the message using the 128-bit established in step 82 and sends a Mobile IP registration reply to the MN 1.
90
If the ESP established is not active, the MN activates the ESP. The MN 2 then sends packets to the target host 8 using the ESP to the PGN 7. The PGN 7 forwards the packets to the target host 8.
91
The target host 8 replies with packets to the PGN 7b.
92
At the conclusion of the data session, the MN 2 terminates the connection with the PGN 7and detaches from the WLAN.
94
When the MN 1 roams back into the GPRS / UMTS network, the MN 1 sends a Mobile IP registration request to the Home Agent hosted in the PGN 7 indicating that it is back on the home network.
96
The MN 1 uses the 128-bit authentication value obtained within this message. The PGN 7 sends a Mobile IP registration reply to the MN 1 using the 128-bit authentication value obtained within this message.
97

Fig. 8B